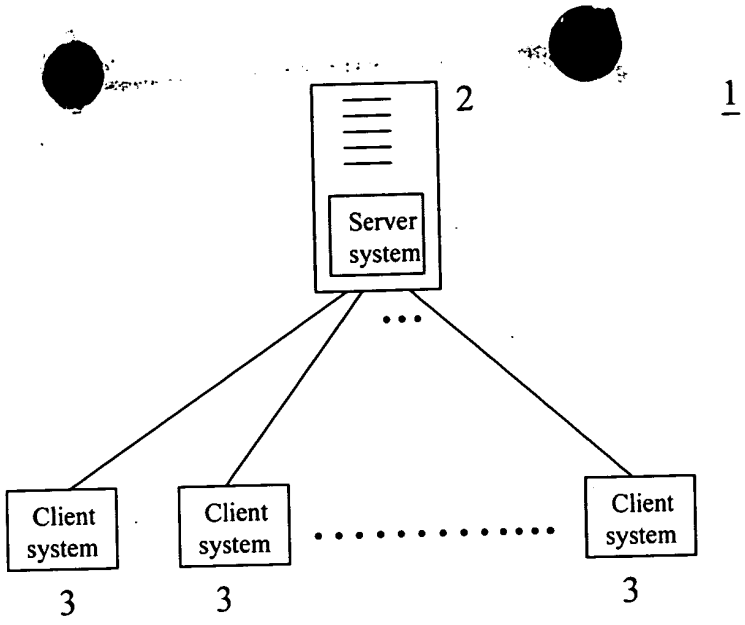
2
1
Server system
Client system
Client system
Client system
3
3
3

Fig. 1

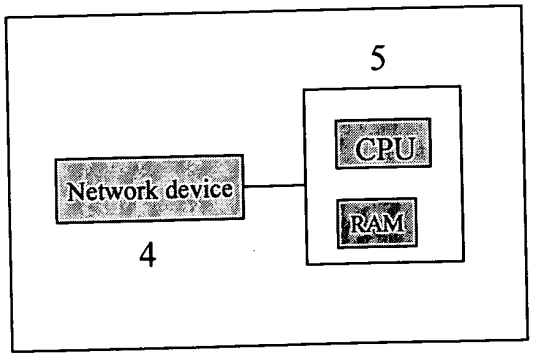
3
5
CPU
RAM
Network device
4

Fig. 2

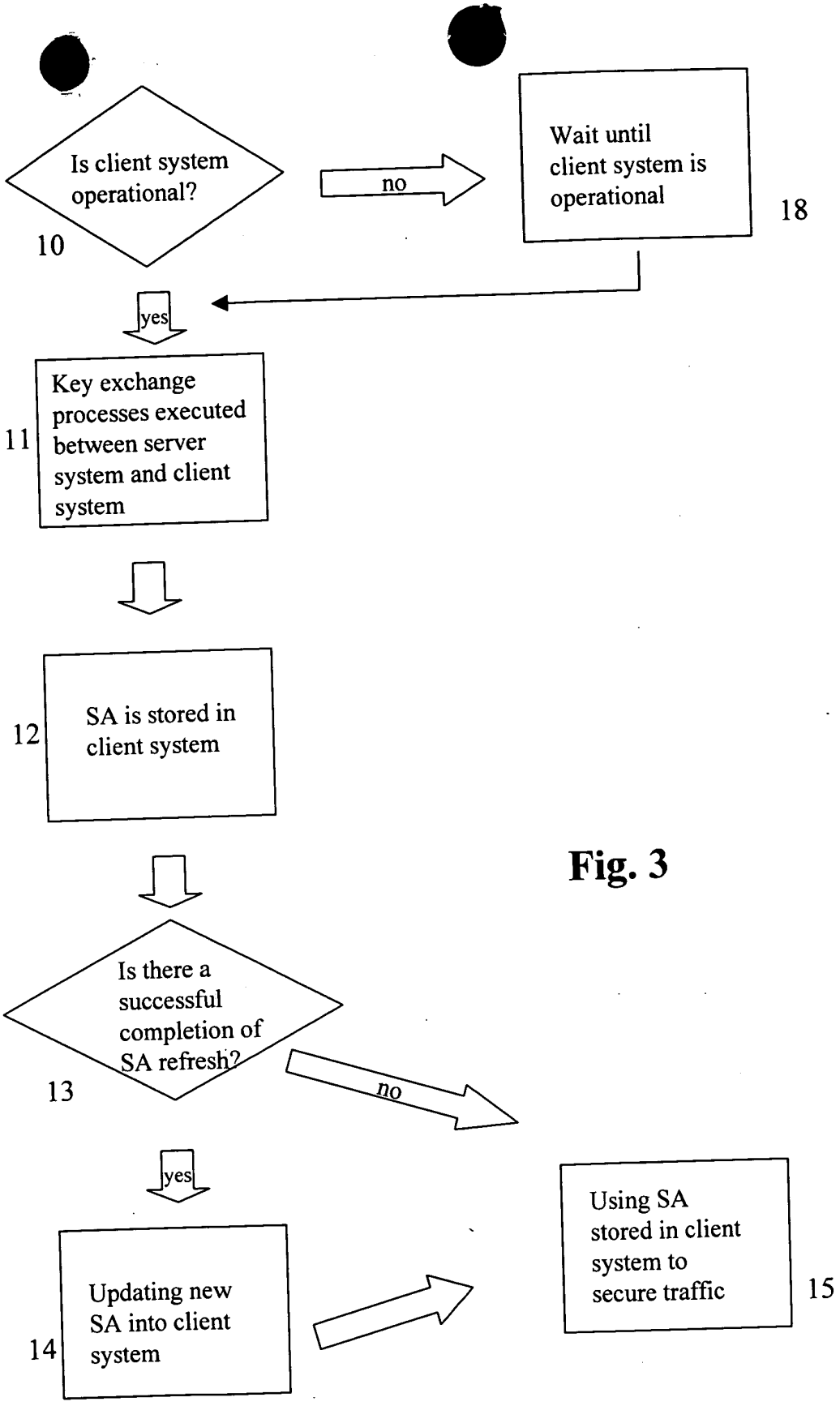
Is client system operational?
10
no
Wait until client system is operational
18
yes
Key exchange processes executed between server system and client system
11
SA is stored in client system
12
Is there a successful completion of SA refresh?
13
no
yes
Updating new SA into client system
14
Using SA stored in client system to secure traffic
15

Fig. 3

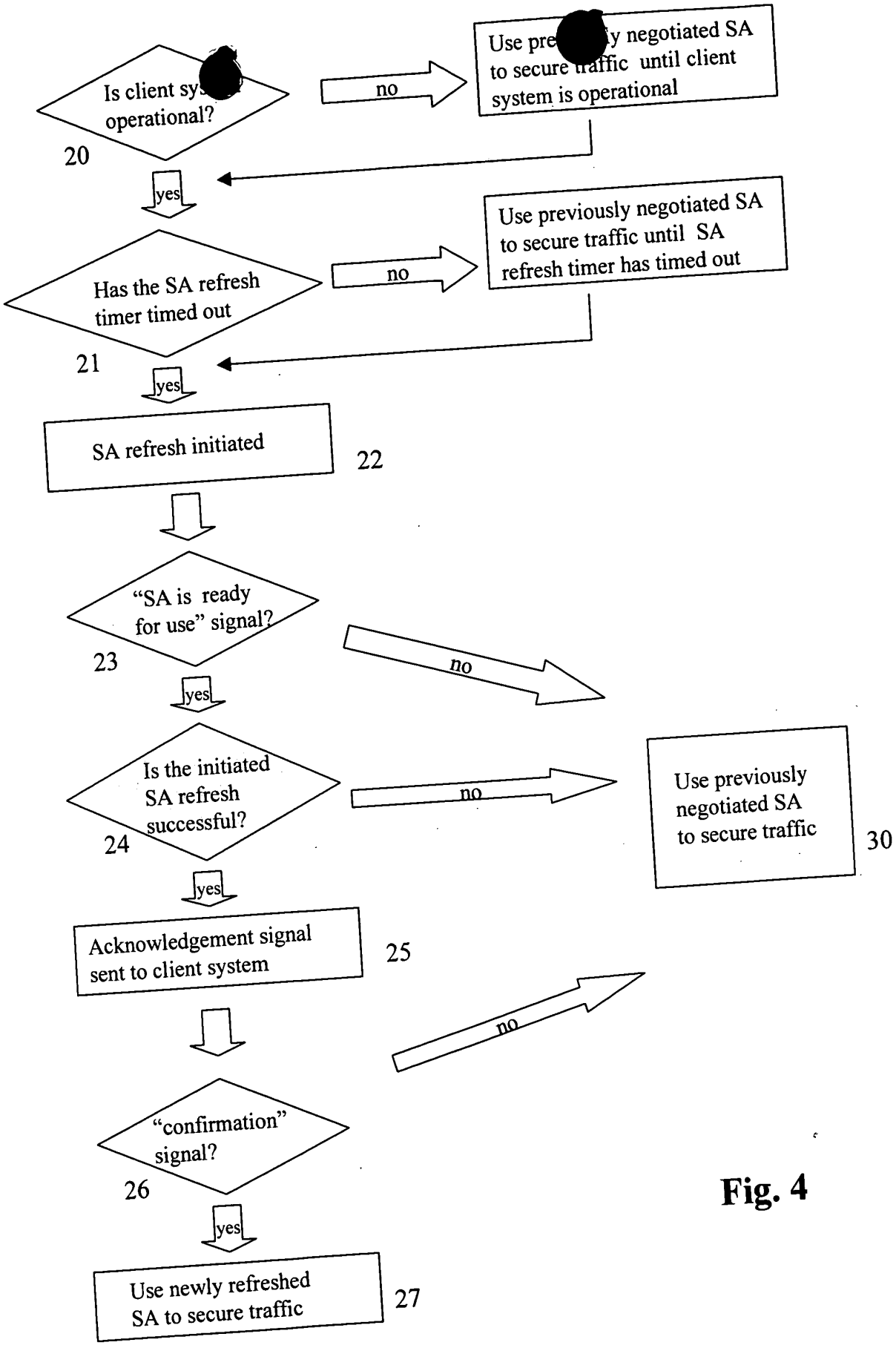
Is client system operational?
20
no
Use previously negotiated SA to secure traffic until client system is operational
yes
Has the SA refresh timer timed out
21
no
Use previously negotiated SA to secure traffic until SA refresh timer has timed out
yes
SA refresh initiated
22
"SA is ready for use" signal?
23
no
yes
Is the initiated SA refresh successful?
24
no
Use previously negotiated SA to secure traffic
30
yes
Acknowledgement signal sent to client system
25
no
"confirmation" signal?
26
yes
Use newly refreshed SA to secure traffic
27

Fig. 4

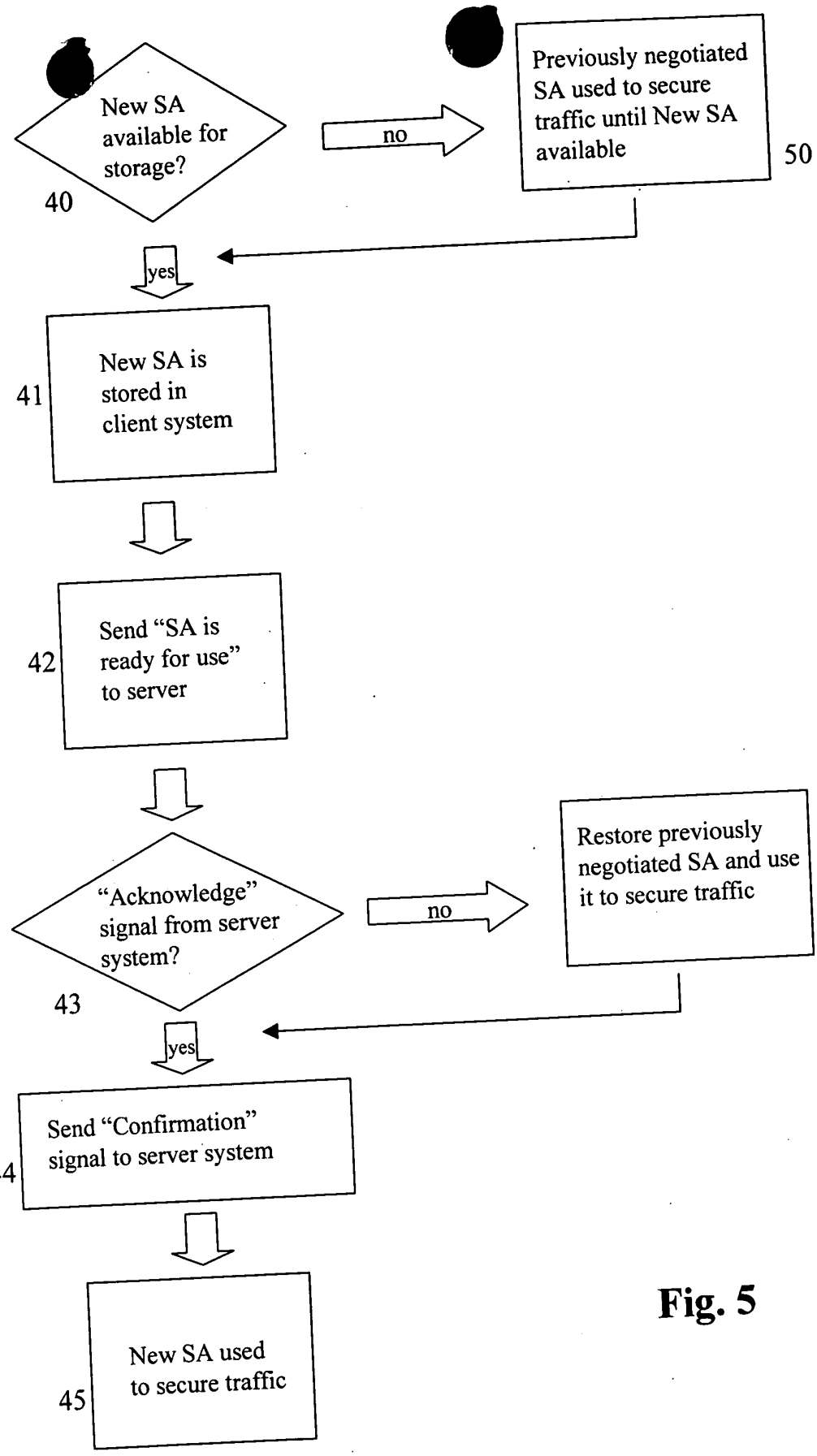
New SA available for storage?
40
no
Previously negotiated SA used to secure traffic until New SA available
50
yes
New SA is stored in client system
41
Send "SA is ready for use" to server
42
"Acknowledge" signal from server system?
43
no
Restore previously negotiated SA and use it to secure traffic
yes
Send "Confirmation" signal to server system
44
New SA used to secure traffic
45

Fig. 5

Fig. 6

State of Client System	State of Server System	Attributes of Transition States
OS up	OS up	IPSec stack on both client and server systems Newly negotiated SA Updated in client system if there is successful completion of SA refresh
OS hung	OS up	IPSec stack not on client system Previously negotiated SA stored in client system is inhibited from being updated
Pre-boot	OS up	IPSec stack not on client system Previously negotiated SA stored in client system is inhibited from being updated
OS suspend	OS up	IPSec stack not on client system Previously negotiated SA stored in client system is inhibited from being updated
Cold-boot	OS up	Client system does not have any security context Configuration option is provided for managing client system without security
Any state	OS hung	Client system is unmanageable by OS hung server system. Fault tolerant system is provided for switching control to secondary server system
OS hung / Pre-boot	Cold Boot	Server system does not have any security context Configuration option is provided for managing client system without security
Cold Boot	Cold Boot	Neither system has any security context Configuration option is provided for allowing traffic to be communicated in the clear